ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

95 SOUTH MARKET ST., SUITE 420
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	December 13, 2005	**Phone Number**	**Fax Number**
To:	Board of Patent Appeals		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P351/01.012.01 **App. No: 09/900,002**

Total Number of Pages Being Transmitted, Including Cover Sheet: 30

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

****
The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone (if long distance, please call collect) and return the original message to us at the above address via the U.S. Postal Service. Thank you.
****

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

December 13, 2005

Practitioner's Docket No. NAI1P351/01.012.01 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Mark J. McArdle et al.

Application No.: 09/900,002 Group No.: 2143
Filed: 07/05/2001 Examiner: Pwu, J.
For: CONTROL OF INTERACTIONS BETWEEN CLIENT COMPUTER APPLICATIONS AND NETWORK RESOURCES

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION–37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on December 13, 2005, which reinstates the appeal originally instated by the Notice of Appeal filed on July 21, 2005, and the original appeal brief filed August 3, 2005.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. ______________ (mandatory)

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273-8300.

Signature

Date: 12/13/2005

Erica L. Farlow
(type or print name of person certifying)

* *Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R.1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$0.00 (previously paid on August 3, 2005)
Total Fee Due	$0.00

6. FEE PAYMENT

Applicant believes that only the above fees are due in connection with the filing of this paper because the appeal brief fee was paid with a previous omission. However, the Commissioner is authorized to charge any additional fees that may be due (e.g. for any reason including, but not limited to fee changes, etc.) to deposit account 50-1351 (Order No. NAI1P351).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. (Order No. NAI1P351).

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:)
)
McArdle et al.) Art Unit: 2143
)
Application No. 09/900,002) Examiner: Pwu, Jeffrey C.
)
Filed: July 5, 2001) Date: December 13, 2005
)
For: CONTROL OF INTERACTIONS BETWEEN)
CLIENT COMPUTER APPLICATIONS AND)
NETWORK RESOURCES)
)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on December 13, 2005, which reinstates the appeal originally instated by the Notice of Appeal filed on July 21, 2005, and the original appeal brief filed August 3, 2005.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION PRESENTED FOR REVIEW

VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appcals, interferences, or related judicial proceedings.

Since no such proceedings exist, no Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-29

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-29
3. Claims allowed: None
4. Claims rejected: 1-29

C. CLAIMS ON APPEAL

The claims on appeal are: 1-29

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1 et al., as shown in Figure 2, a computerized method for restricting network access by applications is provided. In use, a network access request from an application is detected (e.g. item 205 of Figure 2). An application policy file is examined to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network (e.g. item 207 of Figure 2). As a result, access to the network is blocked if the application is not authorized to access the network (e.g. item 209 of Figure 2). Note page 7, line 1-page 8, line 17, for example.

With respect to a summary of Claim 18, the above summary is incorporated, at least in part, by reference. Further, as shown in Figure 3, an application identifier field is provided that contains data identifying an application that is authorized for installation on computer coupled to a network (e.g. item 303 of Figure 3). Also included is a network identifier field that contains data identifying a entity that is accessible by the application identified by the application identifier field (e.g. item 307 of Figure 3). Still yet, an access flag field is included which contains data specifying whether the application identified by the application identifier field is allowed access to the entity identified by the network identifier field (e.g. item 309 of Figure 3). Note page 8, line 18-page 9, line 19, for example.

VI GROUNDS OF REJECTION PRESENTED FOR REVIEW
(37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue #1: The Examiner has rejected Claims 1 and 20 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

Issue #2: The Examiner has rejected Claims 1-29 under 35 U.S.C. 102(e) as being anticipated by Kahn et al., U.S. Patent No. 6,135,646.

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1 and 20 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

Group # 1: Claim 1

The Examiner has argued that Claim 1 is vague and indefinite because it is unclear as to the limitation "detecting a network access request from an application." Specifically, the Examiner alleges that "it is unclear how to request an application based on a detection from a network access or when based on a network access, how to execute, detect, and/or request an application to restrict a network access?"

Appellant does not claim any "request [to] an application based on a detection from a network access or when based on a network access, ... execute, detect, and/or request an application to restrict a network access," but rather merely "detecting a network access request from an application." Clearly, appellant is claiming the detection of a situation where an application requests access to a network.

Group # 2: Claim 20

The Examiner alleges that Claim 20 is vague and indefinite because it is unclear what data or what action is contained in the limitation "containing data specifying an action to perform... if the application identified by the application identifier field attempts access to the entity identified by the network identifier field and the access is not allowed."

Appellant respectfully disagrees, since it is clear that appellant is claiming that the data specifies an action, where the action is that which is performed under a particular condition, namely "if the application identified by the application identifier field attempts access to the entity identified by the network identifier field and the access is not allowed," as claimed.

Issue # 2:

The Examiner has rejected Claims 1-29 under 35 U.S.C. 102(e) as being anticipated by Kahn et al., U.S. Patent No. 6,135,646.

Group # 1: Claims 1, 7, 12, 17, and 29

The Examiner has relied on Col. 8, lines 6-40 and Claim 10 in Kahn to make a prior art showing of appellant's claimed "detecting a network access request from an application" (see this or similar, but not identical language in each of the foregoing claims). Specifically, the Examiner has stated that Kahn discloses a tracking system 46 and detecting and tracking examination of a registration system 40 of registered rights.

Appellant respectfully asserts that such excerpts merely relate to "terms and conditions for use of digital objects and...negotiations with users for rights" (see Col. 8, lines 20-22). Thus, Kahn relates to users accessing digital objects, and not any sort of "network access request from an application," as specifically claimed by appellant (emphasis added).

In addition, the Examiner has relied on Claims 1 and 10 in Kahn to make a prior art showing of appellant's claimed "...to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network" (see this or similar, but not identical language in each of the in claims).

Appellant again respectfully asserts that Kahn merely relates to a user accessing digital objects. In particular, Kahn discloses "the mechanism being arranged to makc the information about terms and conditions available to a user in connection with a request for access to one of the digital objects" (Claims 1 and 10-emphasis added). Appellant, on the other hand, claims "determin[ing] if the application is authorized to access the network" (emphasis added). Furthermore, simply nowhere in Kahn is there even any suggestion of "comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for **installation on computers** coupled to the network" as claimed by appellant (emphasis added).

Still yet, the Examiner has relied on Col. 2, lines 17-47 and Col. 3, lines 14-26 in Kahn to make a prior art showing of appellant's claimed "blocking access to the network if the application is not authorized to access the network" (see this or similar, but not identical language in each of the foregoing claims).

Appellant respectfully asserts that such excerpts from Kahn simply teach blocking access to digital objects, and not to a network, as claimed by appellant. Furthermore, Kahn teaches that "an authorized uscr may have access" (see Col. 2, lines 28-29-emphasis added), but not that an "application is not authorized to access the network," as claimed by appellant (emphasis added).

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. Verdegaal Bros. v. Union Oil Co. Of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. Richardson v. Suzuki Motor Co.868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Kahn reference, since each element as set forth in the claims has not been met, as noted above.

Group #2: Claims 2, 8 and 13

The Examiner has relied on Col. 7, lines 50-60, Col. 8, lines 6-35 and Claims 1 and 10 in Kahn to make a prior art showing of appellant's claimed "determining a network resource requested by the application; examining the application policy file to determining if the application is authorized to access the network resource; and allowing access to the network resource if the application is authorized to access the network resource."

Appellant respectfully asserts that that Kahn only teaches "the mechanism being arranged to make the information about terms and conditions available to a user in connection with a request for access to one of the digital objects" (Claims 1 and 10-emphasis added). Thus, Kahn only teaches a user accessing a digital object, and not a "network resource requested by the application" and "determin[ing] if the application is authorized to access the network resource," as claimed by appellant (emphasis added).

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #3: Claims 3, 9 and 14

The Examiner has relied on Col. 7, lines 50-60, Col. 8, lines 6-35 and Claims 1 and 10 in Kahn to make a prior art showing of appellant's claimed "determining a type of network access requested by the application; examining the application policy file to determine if the application is authorized for the type of network access requested; and allowing the type of network access requested if the application is authorized for the type of network access requested."

Again, appellant respectfully asserts that Kahn merely teaches user rights with respect to accessing digital objects, and not application authorizations with respect to a type of network access, in the manner claimed by appellant.

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #4: Claims 4, 10 and 15

The Examiner has relied on Col. 7 lines 50-60, Col. 8, lines 6-35 and Claims 1 and 10 in Kahn to make a prior art showing of appellant's claimed "updating the application policy file; and re-evaluating applications currently executing again the updated policy file." Appellant respectfully asserts that Kahn only relates to user rights to access a digital object, and thus does not even suggest re-evaluating applications currently executing against the updated policy file.

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #5: Claims 5, 11 and 16

The Examiner has relied on Col. 6, lines 22-25 in Kahn to make a prior art showing of appellant's claimed technique "wherein the application identifier is in the network access request." Appellant respectfully asserts that such excerpt merely discloses that a "digital object has a…concise unique identifier." Clearly, an identifier for a digital object does not meet appellant's claimed application identifier, let alone that such "application identifier is in the network access request," as specifically claimed by appellant (emphasis added).

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #6: Claim 6

The Examiner has relied on 14 from Kahn to make a prior art showing of appellant's claimed technique "wherein the method is performed on a client computer on which the application is executing." Appellant assumes that the Examiner was referring to Figure 14. However, appellant notes that Figure 14 only shows a workstation 42, but not specifically that such workstation is "on which the application is executing," as claimed by appellant.

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #7: Claims 18 and 21

The Examiner has relied on Col. 7, lines 50-60, Col. 8, lines 6-35 and Claims 1 and 10 to make a prior art showing of appellant's claimed "application identifier field containing data identifying an application that is authorized for installation on computer coupled to a network; a network identifier field containing data identifying a entity that is accessible by the application identified by the application identifier field; and an access flag field containing data specifying whether the application identified by the application identifier field is allowed access to the entity identified by the network identifier field."

Appellant respectfully asserts that Kahn only discloses "the mechanism being arranged to make the information about terms and conditions available to a user in connection with a request for access to one of the digital objects" (Claims 1 and 10-emphasis added). Thus, Kahn only relates to a user accessing a digital object. Appellant on the other hand, specifically claims "an application that is authorized for installation on computer coupled to a network," "a[n] entity that is accessible by the application," and "data specifying whether the application... is allowed access to the entity" (emphasis added).

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #9: Claim 19

The Examiner has relied on Col. 7, line 50-Col. 8, line 35 in Kahn to make a prior art showing of appellant's claimed "additional policy rule field containing data specifying whether the application identified by the application identifier field is allowed a particular type of access to the entity identified by the network identifier field." Appellant respectfully asserts that such excerpt merely discloses "terms and conditions for use of digital objects and...negotiations with users for rights." Thus, only users are give access to the digital objects, and it is not determined "whether the application... is allowed a particular type of access to the entity," as claimed by appellant (emphasis added).

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #10: Claim 20

The Examiner has failed to even respond to appellant's claimed "response field containing data specifying an action to performed if the application identified by the application identifier field attempts access to the entity identified by the network identifier field and the access is not allowed."

Appellant respectfully asserts that Kahn does not even disclose any sort of action taken if access is not allowed, and thus does not meet appellant's claimed "response field." Furthermore, since Kahn only relates to user permissions with respect to digital objects, Kahn cannot even inherently include "an action to performed if the application... attempts access to the entity... and the access is not allowed," as claimed by appellant (emphasis added).

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #11: Claim 22

The Examiner has relied on Col. 7, lines 50-60, Col.8, lines 6-35 and Claims 1 and 10 in Kahn to make a prior art showing of appellant's claimed technique "wherein the application identifier is selected from the group consisting of a file name of the application and a path on the network." Appellant respectfully asserts that Kahn only relates to "rights in digital objects...and conditions under which they are accessed by users" (see Abstract-emphasis added). Thus, when read in context, appellant's claimed application identifier is that which itself accesses the network such that a file name of the application or a path on the network identify the application accessing the network. Clearly, appellant's claimed "application identifier" is not met by Kahn since Kahn only teaches a user that accesses a digital object.

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #12: Claim 23

The Examiner has relied on Col. 7, lines 50-60, Col. 8, lines 6-35 and Claims 1 and 10 in Kahn to make a prior art showing of appellant's claimed technique "wherein a plurality of the application identifiers..." However, appellant respectfully asserts that Kahn does not disclose any type of "plurality of the <u>application</u> identifiers," as claimed by appellant (emphasis added).

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group # 13: Claim 24 and 26

The Examiner has relied on Claim 1 in Kahn to make a prior art showing of appellant's claimed technique "wherein each application entry in the application policy file comprises a set of access policy rules for one of a network and a network resource identified by the network identifier." Appellant respectfully asserts that Kahn merely relates to <u>users</u> accessing <u>digital objects</u> (see Abstract), and therefore does not disclose any sort of <u>application policy file</u>, in the context claimed by appellant.

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #14: Claim 25 and 27

The Examiner has relied on Col. 24, lines 34-42 to make a prior art showing of appellant's claimed technique "wherein the network identifier is selected from the group consisting of a network address range and a Universal Naming Convention path."

Appellant respectfully asserts that such excerpt merely relates to a system that requests access to an object in a repository. Furthermore, the only network address disclosed in Kahn relates to the "calling network address" (i.e. the network address of the system requesting access to the object). Clearly, the network address of the system making the request does not meet appellant's claimed "network identifier" since, when read in context, appellant's claimed "network identifier" identifies a "network resource" that itself is accessed by an application.

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

Group #15: Claim 28

The Examiner has relied on Col. 7, lines 50-60, Col. 8, lines 6-35 and Claims 1 and 10 in Kahn to make a prior art showing of appellant's claimed technique "wherein the application policy file includes an application identifier, a network identifier, an access flag, additional policy rules, and at least on application entry."

Appellant respectfully asserts that nowhere in Kahn is there any disclosure of an application policy file, but instead Kahn only teaches "terms and conditions under which [digital objects] are accessed by users in a network" (see Abstract). Thus, Kahn only relates to permissions of users and would therefore not require an "application policy file," and especially not in the specific manner claimed by appellant (emphasis added).

Again, each element as set forth in the claims has not been met by the Kahn reference, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computerized method for restricting network access by applications comprising:

detecting a network access request from an application;

examining an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network; and

blocking access to the network if the application is not authorized to access the network.

2. (Original) The method of claim 1 further comprising:

determining a network resource requested by the application;

examining the application policy file to determine if the application is authorized to access the network resource; and

allowing access to the network resource if the application is authorized to access the network resource.

3. (Original) The method of claim 1 further comprising:

determining a type of network access requested by the application;

examining the application policy file to determine if the application is authorized for the type of network access requested; and

allowing the type of network access requested if the application is authorized for the type of network access requested.

4. (Original) The method of claim 1 further comprising:

updating the application policy file; and

re-evaluating applications currently executing against the updated policy file.

5. (Previously Amended) The method of claim 1, wherein the application identifier is in the network access request.

6. (Original) The method of claim 1, wherein the method is performed on a client computer on which the application is executing.

7. (Previously Presented) A computer-readable medium having executable instruction to cause a computer to perform a method comprising:

detecting a network access request from an application;

examining an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network; and

blocking access to the network if the application is not authorized to access the network.

8. (Original) The computer-readable medium of claim 7, wherein the method further comprises:

determining a network resource requested by the application;

examining the application policy file to determine if the application is authorized to access the network resource; and

allowing access to the network resource if the application is authorized to access the network resource.

9. (Original) The computer-readable medium of claim 7, wherein the method further comprises:

determining a type of network access requested by the application;

examining the application policy file to determine if the application is authorized for the type of network access requested; and

allowing the type of network access requested if the application is authorized for the type of network access requested.

10. (Original) The computer-readable medium of claim 7, wherein the method further comprises:

updating the application policy file; and

re-evaluating applications currently executing against the updated policy file.

11. (Previously Presented) The computer-readable medium of claim 7, wherein thc application identifier is in the network access request.

12. (Previously Presented) A computer system comprising:

a processing unit;

a memory coupled to the processing unit through a bus;

a network interface coupled to the processing unit through the bus and further operable for coupling to a network; and

an application policy process executed from the memory by the processing unit to cause the processing unit to detect a network access request from an application, to examine an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network, and to block access to tbe network if the application is not authorized to access the network.

13. (Original) The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a network resource requested by the application, to examine the application policy file to determine if the application is authorized to access the network resource, and to allow access to the network resource if the application is authorized to access thc network resource.

14. (Original) The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a type of network access requested by the application, to examine the application policy file to determine if the application is authorized for the type of network access requested, and to allow the type of network access requested if the application is authorized for the type of network access requested.

15. (Original) The computer system of claim 12, wherein the application policy process further causes the processing unit to update the application policy file, and to re-evaluate applications currently executing against the updated policy file.

16. (Previously Amended) The computer system of claim 12, wherein the application identifier is in the network access request.

17. (Original) The computer system of claim 12, wherein the application is executed from the memory by the processing unit.

18. (Previously Presented) A computer-readable medium having stored thereon an application policy data structure comprising:

an application identifier field containing data identifying an application that is authorized for installation on computer coupled to a network;

a network identifier field containing data identifying a entity that is accessible by the application identified by the application identifier field; and

an access flag field containing data specifying whether the application identified by the application identifier field is allowed access to the entity identified by the network identifier field.

19. (Original) The computer-readable medium of claim 18 further comprising:

an additional policy rule field containing data specifying whether the application identified by the application identifier field is allowed a particular type of access to the entity identified by the network identifier field.

20. (Original) The computer-readable medium of claim 18 further comprising:

a response field containing data specifying an action to performed if the application identified by the application identifier field attempts access to the entity identified by the network identifier field and the access is not allowed.

21. (Original) The computer-readable medium of claim 18, wherein the entity is selected from the group consisting of a network and a network resource.

22. (Previously Presented) The method of claim 5, wherein the application identifier is selected from the group consisting of a file name of the application and a path on the network.

23. (Previously Presented) The method of claim 5, wherein a plurality of the application identifiers are associated with each application, and each of the application identifiers corresponds to a different network address assigned to the corresponding application.

24. (Previously Presented) The method of claim 1, wherein each application entry in the application policy file comprises a set of access policy rules for one of a network and a network resource identified by a network identifier.

25. (Previously Presented) The method of claim 24, wherein the network identifier is selected from the group consisting of a network address range and a Universal Naming Convention path.

26. (Previously Presented) The method of claim 24, wherein the set of access policy rules includes a first rule that allows DNS service from a specified network server, and a second rule that disallows FTP with respect to specified addresses.

27. (Previously Presented) The method of claim 26, wherein a null setting for an access flag is interpreted as one of allowing and disallowing all access to a network specified by the network identifier.

28. (Previously Presented) The method of claim 1 wherein the application policy file includes an application identifier, a network identifier, an access flag, additional policy rules, and at least one application entry.

29. (Previously Presented) A computerized method for execution on a computer coupled to a network to restrict network access by an application executing on the computer, the method comprising:

detecting a network request from the application, the request comprising at least one of an identifier and entity and a type of network access, wherein the entity is one of a network and a network resource;

examining an application policy file to determine if the application is authorized to access the entity by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network, wherein each application entry in the application policy file comprises a set of access policy rules for a network corresponding to a network identifier, the network identifier comprising at least one of a network address range and a Universal Naming Convention path, and wherein the application policy file further comprises an access flag having a null setting that is interpreted as one of allowing and disallowing all access to a network specified by the network identifier;

blocking access to the entity if the application is not authorized to access the entity; and

re-evaluating applications currently executing against any updated application policy file,

wherein a plurality of the application identifiers are associated with each application, each application identifier corresponding to a different network address assigned to the corresponding application, and wherein each application identifier is one of a file name of the application and a path on the network.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P351_01.012.01).

Respectfully submitted,

By: ____________________ Date: 12/13/05

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660